(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number : **0 677 801 A1**

(12) EUROPEAN PATENT APPLICATION

(21) Application number : **95302117.7**

(51) Int. Cl.[6] : **G06F 1/00,** G07C 9/00

(22) Date of filing : **29.03.95**

(30) Priority : **04.04.94 US 223252**

(43) Date of publication of application :
18.10.95 Bulletin 95/42

(84) Designated Contracting States :
DE ES FR GB IT

(71) Applicant : **AT & T Corp.**
32 Avenue of the Americas
New York, NY 10013-2412 (US)

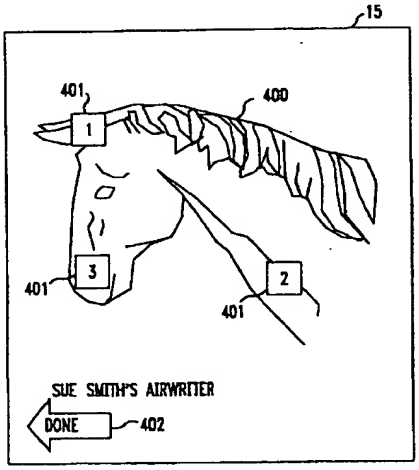
(72) Inventor : **Blonder, Greg E.**
112 Mountain Avenue
Summit, New Jersey 07901 (US)

(74) Representative : **Watts, Christopher Malcolm Kelway, Dr. et al**
AT&T (UK) Ltd.
5, Mornington Road
Woodford Green Essex, IG8 0TU (GB)

(54) Graphical password.

(57) A graphical password arrangement displays a predetermined graphical image (400) and requires a user to "touch" predetermined areas (401) of the image in a predetermined sequence, as a means of entering a password.

FIG. 4



EP 0 677 801 A1

Technical Field

This invention relates generally to processing systems and specifically relates to resource-access control arrangements such as password arrangements.

Background of the Invention

The use of passwords to control access to resources such as computers, databases, telecommunications facilities, etc., is well known and understood. Before being given access to a requested resource, a user is required to enter a valid password as a way of ensuring that the user is authorized to access the resource. Normally, the password is a word or some other sequence of alphanumeric characters. The normal method of entry is to speak the word into a microphone or to key the sequence of characters in on a terminal or a telephone keyboard.

Conventional alphanumeric passwords suffer from disadvantages, however. Firstly, they are difficult for the users to remember, particularly if they are arbitrary alphanumeric sequences rather than normal words. Secondly, they are relatively easy to compromise, particularly by the use of a computer that is programmed to automatically try all dictionary words or all permutations of some number of alphanumeric characters as passwords in an attempt to gain unauthorized access to a resource.

To overcome these difficulties, recently new security arrangements have been developed that rely on sensing of a user's individual and not readily duplicated characteristics as a means of validating the user's identity. These include voice analyzers, retina scanners, fingerprint image analyzers, and face image analyzers. While quite effective in overcoming the disadvantages associated with conventional alphanumeric passwords, these arrangements have disadvantages of their own. Chief amongst them is their complexity and associated cost, which make their use impractical for most of applications.

Summary of the Invention

This invention is directed to overcoming these and other problems and disadvantages of the prior art. Generally according to the invention, there is provided a graphical password arrangement, wherein a user seeking access to a resource is presented with a predetermined image on a visual display and is required to point to (e.g. touch) one or more predetermined positions on the displayed image (referred to herein as "tap regions") in a predetermined order as a way of indicating his or her authorization to access the resource.

Specifically according to the invention as claimed, there is provided a graphical password arrangement and/or method. The arrangement comprises means for displaying a predetermined image, means for storing a predetermined number of predetermined positions in the predetermined image as a password, means responsive to a user for determining a user's selections of locations in the displayed image, means for determining whether the determined locations selected by the user correspond to the predetermined positions of the password, and means responsive to a determination of a lack of correspondence between the determined locations and the predetermined positions for denying the user access to a resource that is protected by the password. The method correspondingly comprises the steps of displaying a predetermined image, selecting locations in the displayed image under user control, determining whether the selected locations correspond to a predetermined number of predetermined positions in the predetermined image that are stored as a password, and denying the user access to the resource in response to a determination that correspondence is lacking between the selected locations and the predetermined positions.

The invention possesses numerous advantages over the prior art. Firstly, people generally find images to be easier to recall than alphanumeric sequences, particularly images with personal meaning. Secondly, even a very coarse matrix of tap regions yields great security. For example, in an arrangement that uses a 3 inch-by-5 inch (7.5 cm -by- 12.5 cm) display with one-quarter inch square (6 mm -by- 6 mm) tap regions and that requires the user to touch three tap regions in the correct order, there are 13.6 million possible combinations. In comparison, a four-digit password like a personal identification number (PIN) is one of only 10,000 possible combinations, and a three-letter password is one of only 17,000 possible combinations. Thirdly, in equipment that already includes a touch-sensitive or a graphics display, the graphical password arrangement is substantially no more difficult or expensive to implement than a conventional password arrangement. But even if the cost and complexity of a touch-sensitive or graphics display and associated software is factored in, the graphical password may be simpler and less costly to implement than the new security arrangements that were mentioned above.

These and other advantages and features of the invention will become more apparent from the following description of an illustrative embodiment of the invention taken together with the drawing.

Brief Description of the Drawing

FIG. 1 is a block diagram of an exemplary processing system that includes an illustrative embodiment of the invention;

FIG. 2 is a flow diagram of a password function

of a PASSWD arrangement of the system of FIG. 1;

FIG. 3 is a flow diagram of a password change function of the PASSWD arrangement of the system of FIG. 1;

FIG. 4 is an illustrative view of a display of the system of FIG. 1 during execution of the function of FIG. 3; and

FIG. 5 is an illustrative view of the display of the system of FIG. 1 during execution of the function of FIG. 2.

Detailed Description

FIG. 1 shows a general diagram of a processing system 10. Processing system may be any one of a wide variety of systems, such as a personal computer, a telecommunications terminal, a personal digital assistant, an entrance security system, a vehicle ignition control system, etc. Processing system 10 is a program-controlled system. It includes a memory 12 that stores control programs and associated data, and a processor 11 that executes the programs. As is often conventional with such systems, processing system 10 also includes a visual display screen 15 and one or more entry devices 14 (such as a keyboard, a mouse, and/or a light pen or a touch pen) that are coupled to processor 11 by an input and output (I/O) interface 13. Display 15 may be a touch-sensitive display screen, and hence itself may function as one of the entry devices 14. As described so far, processing system 10 and its component elements 11-15 are conventional.

Processing system 10 includes a graphical password arrangement PASSWD 16, which in this illustrative example is implemented via a program and data stored in memory 12, and which controls user access to the application capabilities provided by processing system 10. The functionality of PASSWD 16 is represented in flowchart form in FIGS. 2 and 3.

Processing system 10 is initially provided to the user with the password function disabled. Upon power-up of system 10, execution of PASSWD 16 is invoked, at step 200 of FIG. 2, and PASSWD 16 checks whether the password function is enabled, at step 202. If the password function is not enabled, PASSWD 16 grants the user unconditional access to processing system 10 and ceases execution, at step 204.

While using processing system 10, the user may request enablement of the password function or a new password by entering the proper command through an entry device 14. In response, execution of PASSWD 16 is invoked, at step 300 of FIG. 3, and PASSWD 16 prompts the user to provide a password image, at step 302. The user may provide an image in any one or more ways, such as by composing an image on display 15 via one or more entry devices 14, scanning in an existing image via an entry device 14, or selecting one from among a plurality of images that have been loaded and stored in memory 12. PASSWD 16 receives the password image provided by the user and stores it in memory 12, at step 304. It then displays the password image on display 15, at step 306.

Alternatively, the password image may be predefined, and PASSWD 16 skips steps 302 and 304 and proceeds from step 300 directly to step 306.

Following step 306, PASSWD 16 prompts the user to select the size and the number of tap regions that will make up the graphical password, at step 308. Tap regions are positions in the displayed password image. Illustratively, each tap region is a rectangle no larger than 10% of the password image size, and the graphical password consists of at least two tap regions. In response to receiving the user's selection, at step 310, PASSWD 16 displays the selected number of sequentially-numbered tap regions of the selected size along with the password image, at step 312. The tap regions may be displayed in a row along an edge of display 15, or arbitrarily positioned over the password image.

Alternatively, the number and size of tap regions may be predefined, and PASSWD 16 skips steps 308 and 310 and proceeds directly from step 306 to step 312.

An illustrative example of the state of display 15 following step 312 is shown in FIG. 4, where numeral 400 designates the password image and numeral 401 designates the tap regions.

Following step 312, PASSWD 16 prompts the user to select a tap region 401 and to position it within password image 400, at step 314. The user performs these functions via one or more entry devices 14, such as by manipulating a cursor via a keyboard, pointing and dragging the cursor with a mouse, or tapping and sliding on display 15 with a light pen or a touch pen. If display 15 is a touch-sensitive screen, the user may perform the functions by tapping and sliding on display 15 with a finger. PASSWD 16 waits until the user makes a location selection on display 15 via an entry device 14, at step 316, and determines the coordinates of the selected location, at step 318. It then determines whether the entry device 14 is located on a tap region 401, that is, whether a tap region 401 has been properly selected, at step 320. If not, PASSWD 16 returns to step 314 to repeat the instructions to the user.

If it is determined at step 320 that a tap region 401 has been properly selected, PASSWD 16 tracks the movement of entry device 14 across display 15 and moves the selected tap region 401 along with the entry device 14, at step 322, while checking for release of the selected tap region 401 by entry device 14, at step 324. Hence, entry device 14 serves to move the tap region 401 relative to the displayed predeter-

mined image 400. When it determines that entry device 14 has released the selected tap region 401, PASSWD 16 stores the sequence number of the selected tap region 401 and the position coordinates of the location within password image 400 where it had been released, at step 326. PASSWD 16 then checks whether the user has indicated completion of password selection, at step 330. Illustratively, in the example of FIG. 3, the user may indicate completion of password selection by selecting a displayed "done" indicator 402 via entry device 14. If the user has not indicated completion, PASSWD 16 returns to step 316 to await re-selection of a tap region 401. If the user has indicated completion, PASSWD 16 marks the stored tap region sequence numbers and position coordinates in memory 12 as the new password, at step 332, enables the password function, at step 334, and then ends its execution, at step 336.

Alternatively, step 334 may be performed not by PASSWD 16 but manually by a user, via interaction with a separate control function of processing system 10.

Returning to FIG. 2, the next time that processing system 10 is powered up, execution of PASSWD 16 is again invoked at step 200, and this time PASSWD 16 determines at step 202 that the password function is enabled. In response, PASSWD 16 retrieves and displays on display 15 the stored password image 400 without also displaying tap regions 401, at step 206. An illustrative example of the state of display 15 following step 206 and corresponding to FIG. 4 is shown in FIG. 5. PASSWD 16 also retrieves the total number of tap regions 401 that make up the password, at step 208. PASSWD 16 then waits until the user makes a location selection on display 15 with entry device 14, at step 210, and it obtains and stores the coordinates of the selected location, at step 212. Hence, entry device 14 serves to identify, under the user's control, the location selected by the user. Following a selection, PASSWD 16 checks whether the number of selected locations equals the number of tap regions 401 that make up the password, at step 214. If not, PASSWD 16 returns to step 210 to await another sequential selection; if so, PASSWD 16 proceeds to compare the coordinates of each sequentially-selected location against the coordinates of the positions of the corresponding sequentially-numbered tap region 401 within the password image 400 to determine if the selected location lies within the corresponding tap region 401, at steps 216-220. If it is determined at step 218 that the sequence of selected locations sequentially corresponds to the sequence of tap regions, entry of the password has been successful, and PASSWD 16 grants the user access to processing system 10 and ends its execution, at step 226.

If each selected location does not lie within the corresponding tap region 401 in password image 400, entry of the password has failed, and PASSWD 16 checks whether a maximum allowed number of tries at entering the password has been exhausted, at step 222. Illustratively, three tries are allowed. If the maximum number of tries has not been exhausted, PASSWD 16 indicates failure to the user and prompts the user to try again, at step 224. PASSWD 16 then returns to step 210 to await the user's set of selections. But if it is determined at step 222 that the maximum number of tries has been exhausted, PASSWD 16 denies the user access to processing system 10, illustratively by turning power off in processing system 10, and ends its execution, at step 228.

Of course, various changes and modifications to the illustrative embodiment described above will be apparent to those skilled in the art. For example, a password may comprise a plurality of different images, with each image containing one (or more) of the tap regions that make up the password. Thus, a different image would be displayed after each tap (i.e., 3 images, one tap/image). Or, the password may additionally require that particular tap regions be tapped at particular times. For example, the graphical image could be a moving image, such as a short cartoon, requiring the user to click and tap at right locations at the right time. Also, the password image could be a blank screen (i.e., no image), requiring the user to just remember the location of the tap regions by "dead reckoning" (presumably using extra-large tap regions). Such changes and modifications can be made without departing from the the scope of the invention and without diminishing its attendant advantages.

Claims

1. A password arrangement including means (15) for displaying a predetermined image (400), CHARACTERISED BY

   means (12:16) for storing a predetermined number of predetermined positions (401) in the predetermined image as a password;

   first means (13, 14, 11:200-212), responsive to a user, for determining a user's selections of locations in the displayed predetermined image;

   second means (16, 11:214-220) for determining whether the determined locations selected by the user correspond to the predetermined positions of the password; and

   means (11:218-228) responsive to a determination of a lack of correspondence between the determined locations and the predetermined positions, for denying the user access to a resource protected by the password.

2. The arrangement of claim 1 wherein

   the denying means include

means (11:218-226) responsive to a determination of correspondence between the determined locations and the predetermined positions, for granting the user access to the resource.

3. The arrangement of claim 1 wherein
the means for displaying include a visual display screen (15) for displaying the predetermined image; and
the first determining include a device (14) for identifying, under user control, locations selected by the user in the displayed image.

4. The arrangement of claim 1 wherein
the predetermined positions (401) have a predetermined size and a predetermined shape; and
the second determining means include
means (11:218) for determining whether the determined locations selected by the user lie within the predetermined positions in the displayed image.

5. The arrangement of claim 1 wherein
the storing means (12:16) further store a predetermined sequence of a predetermined plurality of the predetermined positions;
the first determining means comprise means (11:210-214) for determining a sequence of the user's selections of the locations on the displayed image; and
the second determining means comprise means (11:216-220) for determining whether the sequence of the determined locations selected by the user sequentially corresponds to the sequence of the predetermined positions of the password.

6. The arrangement of claim 1 wherein
the displaying means include
means (15, 11:306-312), responsive to a request of the user, for displaying a number of position indicators along with the predetermined image;
and the arrangement further comprises
third means (14, 11:314-324) responsive to the user for determining a user's positioning of the displayed position indicators in the displayed predetermined image, and
means (11:326-336), responsive to the determined positioning, for storing positions of the position indicators in the displayed image as the predetermined positions in the storing means.

7. The arrangement of claim 6 wherein
the means for displaying include a visual display screen (15) for displaying the position indicators and the predetermined image; and
the third determining means include a device (14) for moving the displayed position indicators on the visual display screen relative to the displayed predetermined image.

8. The arrangement of claim 6 further comprising:
means (12, 11:300-304) responsive to a request of the user, for storing an image designated by the user as the predetermined image; and wherein
the displaying means display the stored image.

9. The graphical password arrangement of claim 1 wherein:
the means for storing comprise
means (16) for storing a predetermined image (400) and a predetermined sequence of a predetermined plurality of predetermined tap regions (401) in the predetermined image as a password, the predetermined tap regions having a predetermined size and a predetermined shape;
the means for displaying comprise
display means (15) for displaying the stored predetermined image;
the first means comprise
means (14) for selecting locations in the predetermined image displayed by display means, under user control, and
means (11:200-212), cooperative with the selecting means, for determining a plurality of locations selected under user control in a sequence in the displayed predetermined image;
the second means comprise
means (11:214-220) for determining whether the selected locations lie within the predetermined tap regions and whether the sequence of the selected locations corresponds to the predetermined sequence of the predetermined tap regions; and
the means for denying comprise
means (11:218-228) responsive to a determination either that the selected locations lie outside of the predetermined tap regions or that the sequence of the selected locations differs from the sequence of the predetermined tap regions, for denying access to a resource protected by the password, and responsive to a determination that the selected locations lie within the predetermined tap regions and the sequence of the selected locations corresponds to the sequence of the predetermined tap regions, for granting access to the resource.

10. The arrangement of claim 1 wherein
the displaying means include
means (11:306-312), responsive to a re-

quest of the user, for displaying the predetermined plurality of sequentially-designated tap regions having the predetermined size and the predetermined shape, along with the predetermined image;

the selecting means include

means (14) for moving the displayed tap regions on the display means relative to the displayed predetermined image, under user control; and

the arrangement further comprises

means (11:316-324) cooperative with the moving means for determining a positioning of the displayed sequentially-designated tap regions in the displayed predetermined image, and

means (11:324-336) responsive to the determined positioning, for storing positions of the sequentially-designated tap regions in the displayed predetermined image as the predetermined sequence of the predetermined tap regions in the storing means.

11. A method of controlling access to a resource protected by a password, CHARACTERISED BY the steps of:

displaying (206) a predetermined image;

selecting locations (210-214) in the displayed image, under user control;

determining (216-219) whether the selected locations correspond to a predetermined number of predetermined positions (401) in the predetermined image that are stored as a password; and

in response to a determination (218) that correspondence is lacking between the selected locations and the predetermined positions, denying (222, 228) the user access to the resource.

FIG. 1

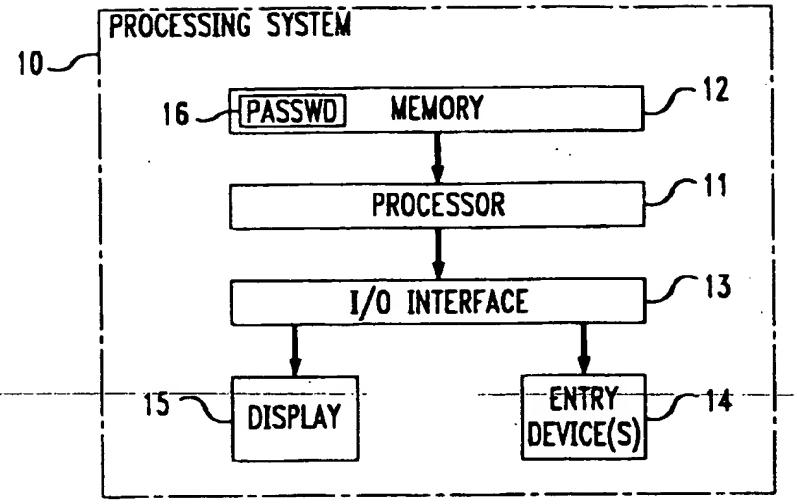

PROCESSING SYSTEM
10
16
PASSWD
MEMORY
12
PROCESSOR
11
I/O INTERFACE
13
15
DISPLAY
ENTRY DEVICE(S)
14

FIG. 2

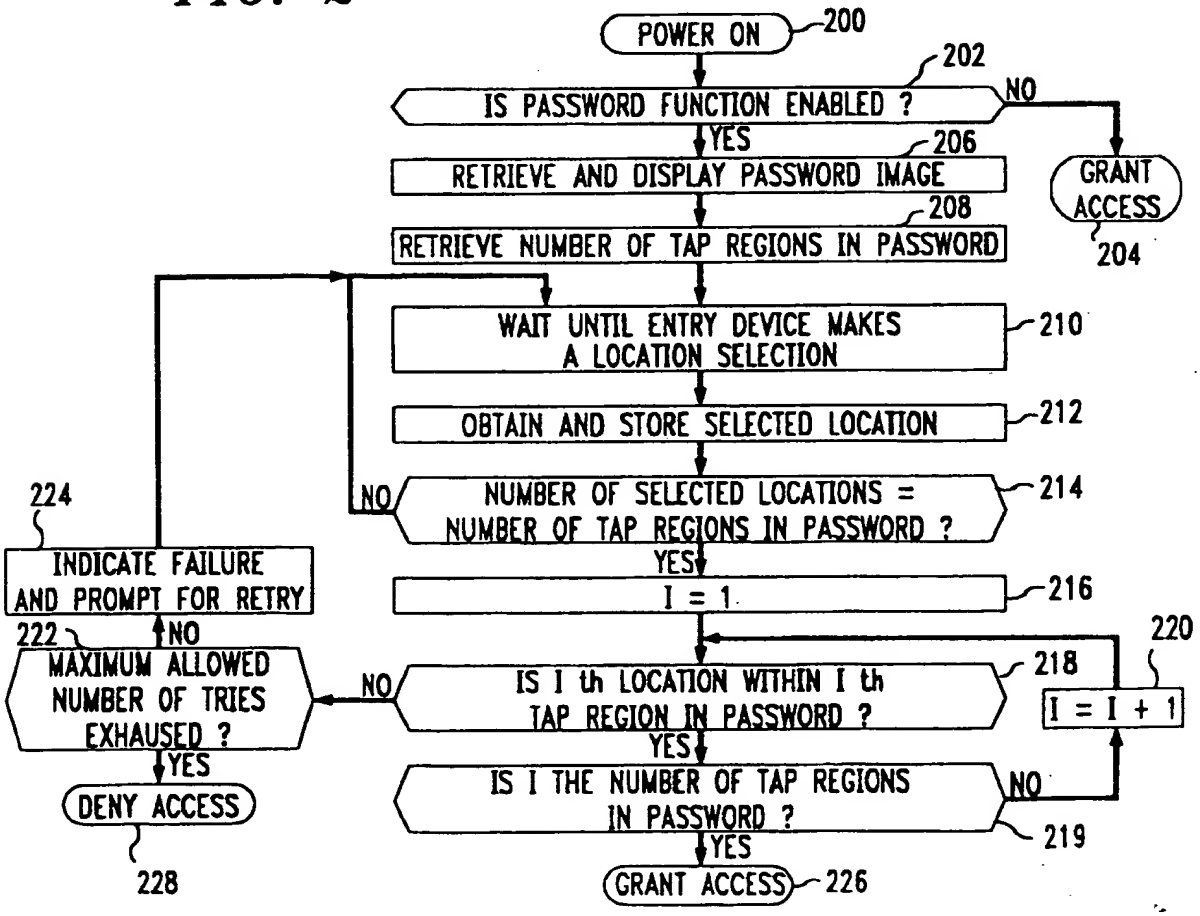

POWER ON
200
IS PASSWORD FUNCTION ENABLED ?
202
NO
YES
GRANT ACCESS
204
RETRIEVE AND DISPLAY PASSWORD IMAGE
206
RETRIEVE NUMBER OF TAP REGIONS IN PASSWORD
208
WAIT UNTIL ENTRY DEVICE MAKES A LOCATION SELECTION
210
OBTAIN AND STORE SELECTED LOCATION
212
NUMBER OF SELECTED LOCATIONS = NUMBER OF TAP REGIONS IN PASSWORD ?
214
NO
YES
I = 1
216
IS I th LOCATION WITHIN I th TAP REGION IN PASSWORD ?
218
NO
YES
I = I + 1
220
IS I THE NUMBER OF TAP REGIONS IN PASSWORD ?
219
NO
YES
GRANT ACCESS
226
INDICATE FAILURE AND PROMPT FOR RETRY
224
MAXIMUM ALLOWED NUMBER OF TRIES EXHAUSED ?
222
NO
YES
DENY ACCESS
228

FIG. 3

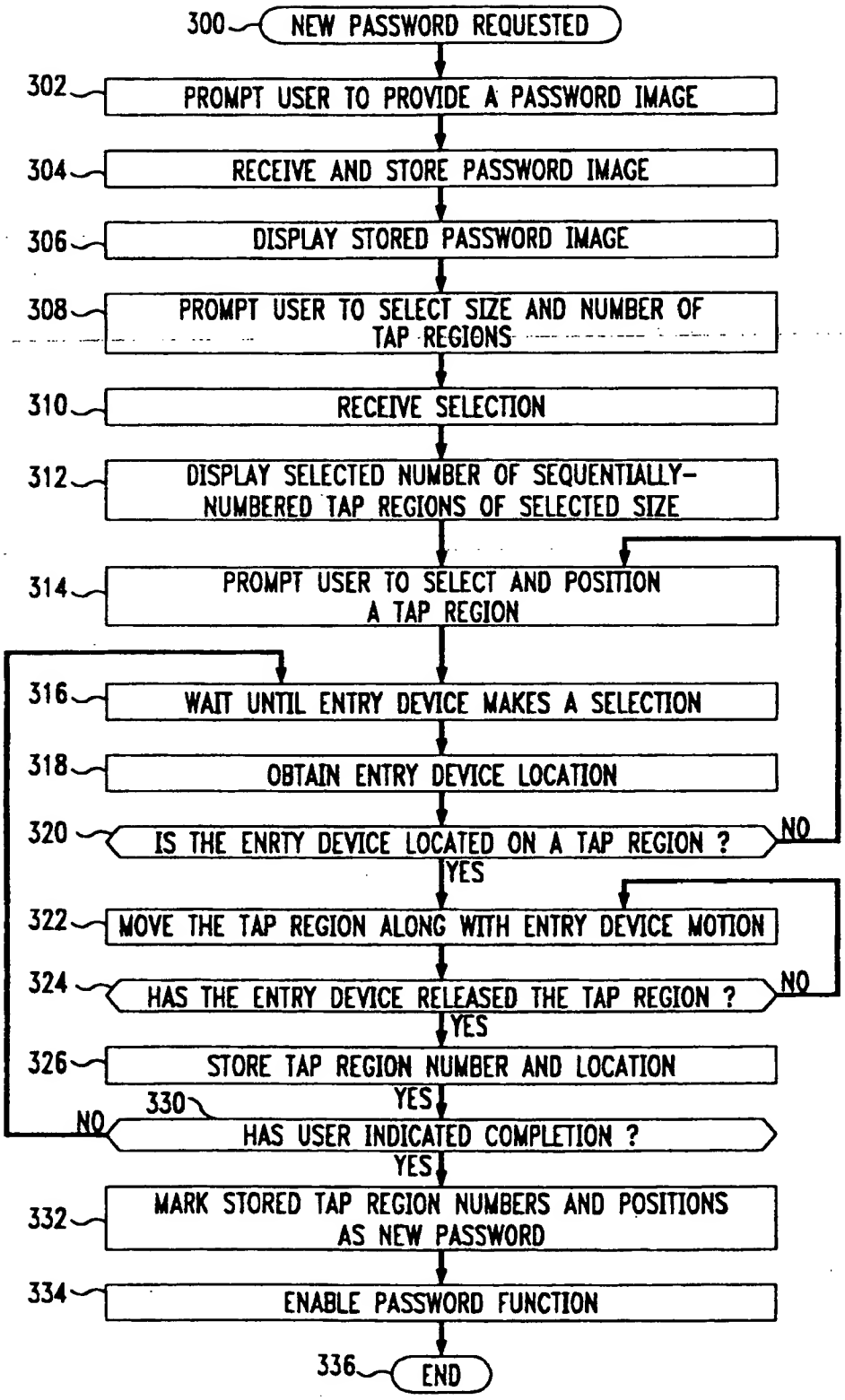

300
NEW PASSWORD REQUESTED
302
PROMPT USER TO PROVIDE A PASSWORD IMAGE
304
RECEIVE AND STORE PASSWORD IMAGE
306
DISPLAY STORED PASSWORD IMAGE
308
PROMPT USER TO SELECT SIZE AND NUMBER OF TAP REGIONS
310
RECEIVE SELECTION
312
DISPLAY SELECTED NUMBER OF SEQUENTIALLY-NUMBERED TAP REGIONS OF SELECTED SIZE
314
PROMPT USER TO SELECT AND POSITION A TAP REGION
316
WAIT UNTIL ENTRY DEVICE MAKES A SELECTION
318
OBTAIN ENTRY DEVICE LOCATION
320
IS THE ENRTY DEVICE LOCATED ON A TAP REGION ?
NO
YES
322
MOVE THE TAP REGION ALONG WITH ENTRY DEVICE MOTION
324
HAS THE ENTRY DEVICE RELEASED THE TAP REGION ?
NO
YES
326
STORE TAP REGION NUMBER AND LOCATION
330
YES
NO
HAS USER INDICATED COMPLETION ?
YES
332
MARK STORED TAP REGION NUMBERS AND POSITIONS AS NEW PASSWORD
334
ENABLE PASSWORD FUNCTION
336
END

FIG. 4

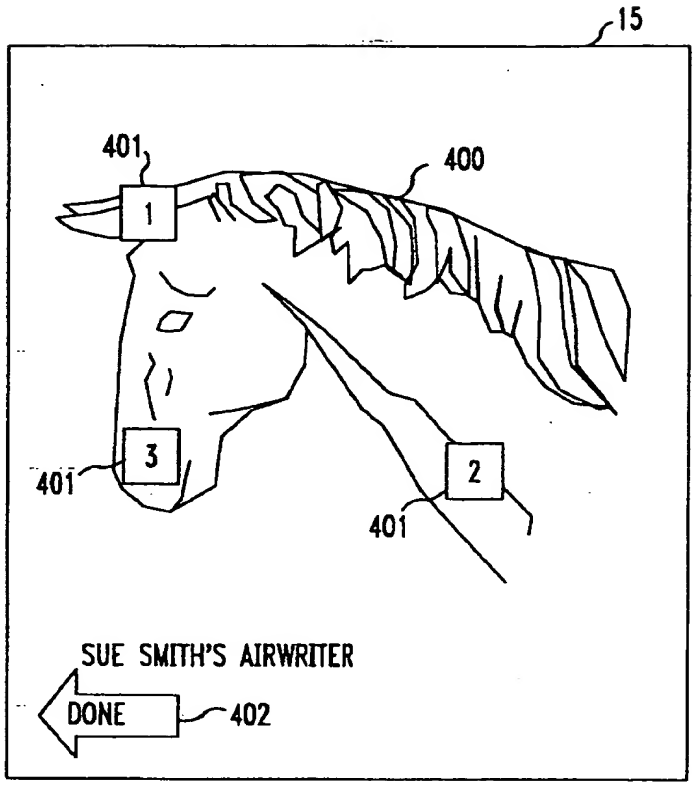
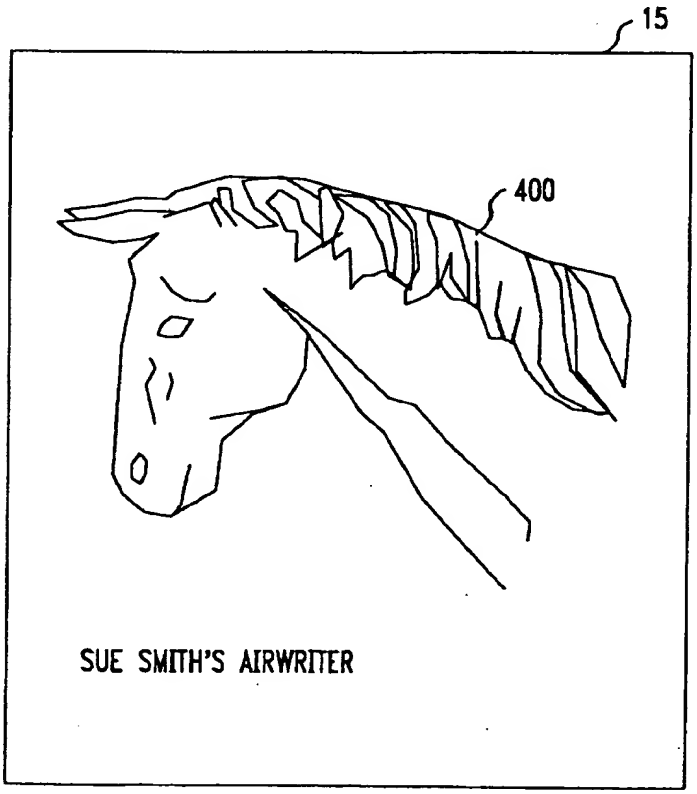

15
401
400
1
3
401
2
401
SUE SMITH'S AIRWRITER
DONE
402

FIG. 5


15
400
SUE SMITH'S AIRWRITER

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 95 30 2117

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
X	IBM TECHNICAL DISCLOSURE BULLETIN, vol. 32, no. 10B, March 1990 NEW YORK US, pages 463-464, 'MENU ICON WITH HIDDEN GEOMETRICAL PASSWORD'	1-5,11	G06F1/00 G07C9/00
A	* page 463, paragraph 1 - paragraph 3 *	6-10	
A	WO-A-93 11511 (DAVIES) * page 8, line 28 - page 9, line 21 * * page 14, line 15 - line 25 *	1,11	

TECHNICAL FIELDS SEARCHED (Int.Cl.6)

G06F
G07C

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	8 August 1995	Moens, R

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)